UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/669,352	09/26/2000	Stephen A. Bagshaw	ATI000092	4574

34456 7590 05/06/2004

TOLER & LARSON & ABEL L.L.P.
5000 PLAZA ON THE LAKE STE 265
AUSTIN, TX 78746

EXAMINER	
HO, THOMAS M	
ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 05/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/669,352	**Applicant(s)** BAGSHAW, STEPHEN A.
	Examiner Thomas M Ho	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on 26 September 2000.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-35 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-35 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 6, 8, 9, 21, 22, 23, 33, 34 are rejected under 35 U.S.C. 112 2nd paragraph as being indefinite.

3. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "orthogonal" in claims 6, 8, 9, 21, 22, 23, 33, 34 is used by the claim to appear to mean "dynamically changeable", while the accepted meaning is

- **or·thog·o·nal** Pronunciation Key (ôr-thŏg'ə-nəl)
  adj.
- Relating to or composed of right angles.
- *Mathematics.*
  - Of or relating to a matrix whose transpose equals its inverse.

  - Of or relating to a linear transformation that preserves the length of vectors.

- \Or*thog"o*nal\, a. [Cf. F. orthogonal.] Right-angled; rectangular; as, an orthogonal intersection of one curve with another.

- N mutually orthogonal vectors span an N-dimensional vector space, meaning that, any vector in the space can be expressed as a linear combination of the vectors. This is true of any set of N linearly independent vectors. The term is used loosely to mean mutually independent or well separated. It is used to describe sets of primitives or capabilities that, like linearly independent vectors in geometry, span the entire "capability space" and are in some sense non-overlapping or mutually independent. For example, in logic, the set of operators "not" and "or" is described as orthogonal, but the set "nand", "or", and "not" is not (because any one of these can be expressed in terms of the others).

  Also used loosely to mean "irrelevant to", e.g. "This may be orthogonal to the discussion, but ...", similar to "going off at a tangent".

The term is indefinite because the specification does not clearly redefine the term. On page 6 2nd paragraph, applicant appears to refer as encoded transmissions between two parties through a mathematical transformation such as an orthogonal transform involving the PCI key. Applicant appears to suggest one example of such an orthogonal transform:

"In one embodiment, an exclusive OR (XOR) calculation is performed between the data to be transmitted and the PCI key to encode transmission but fails to specifically define such a term.

The examiner notes that those of ordinary skill in the art would recognize that XOR maintains a special significance as the fundamental function behind the one-time-pad, a theoretically unbreakable encryption because every outcome to the encryption is equally likely. No amount of frequency analysis can ever break this.

From the definition to orthogonal as may be construed from above, the two closest definitions, compared with the applicant's suggested meaning is "non-overlapping or mutually independent", and in mathematics "perpendicular". Examiner has failed to specifically uncover any such meaning specifically related to encryption.

However, for the purposes of examination and based on the closest mathematical definitions found, the Examiner shall take "orthogonal" in the context of the phrase "orthogonal encryption" to mean, an encryption by which the output is shuffled and unidentifiable from the input text, such that output encryption is completely random or has achieved the greatest point of unidentifiability, such as that which can be produced by a one-time-pad.

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 6, 8, 9, 21, 22, 23, 33, 34 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As noted above, the examiner has taken the term orthogonal in the context used by the applicant to refer to an encryption by which the output is shuffled and unidentifiable from the input text, such that output encryption is completely random or has achieved the greatest point of unidentifiability, such as that which can be produced by a one-time-pad.

The examiner notes however, that if this is the case, the *only* functions capable of producing true orthogonality are one-time-pads- or variants thereof. It is known to those of ordinary skill in the art, that the difficulty implementing a one-time-pad in the art, is not the complexity of the functions, but in the implementation of a true random number generator required. It is known in the art that unless a truly random number is used, the encryption provided by a one-time-pad is woefully inadequate. Applicant fails to sufficiently address the implementation of such a RNG.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-9, 12-16, 21-23 are rejected under 35 U.S.C. 102(a) as being anticipated by Patel, US Patent 6,243,811.

In reference to claim 1:

Patel (Column 4, lines 1-11) discloses a method comprising:

- Establishing an encrypted link between a peripheral device and a software component of an information handling system, wherein establishing the encrypting link includes generating a first seed key common to both the peripheral device and the software component., where the peripheral device is the mobile unit, the software component of the information handling system is the software of the AC, the first seed key is M-Key, which is common to both the mobile unit and the AC.
- Providing the first seed key and a public encryption key associated with the peripheral device to a hardware controller, where the public encryption key is the A-key which is unique to the hardware controller, the HLR, and the peripheral, the mobile. (Column 4, lines 1-11)
- Generating in the hardware controller, using the first seed key and the public encryption key, a second seed key different from the first seed key, the second key to encrypt communications between the software component and the

hardware controller, where the SSD generated is the second seed key generated from the A-key and the M-key. (Column 1, lines 55-64)

In reference to claim 2:

Patel(Column 4, lines 1-4) discloses a method wherein generating the first seed key is performed by the software component, where the software component is the software that executes on the AC/HLR and where the first seed key is M-key.

In reference to claim 3:

Patel (Column 2, lines 22-30) discloses a method wherein generating the first seed key includes:

- Using the public encryption key(A-Key) associated with the peripheral device(the Mobile) to select a plurality of private encryption keys associated with the software component(AC/HLR), where the private encryption keys are SSDA and SSDB
- Determining the seed key based upon the selected private keys associated with the software component, where Patel discloses that the seed key SSD is based upon the selected private keys SSDA and SSDB.

In reference to claim 4:

Patel(Column 4, lines 1-4) discloses a method wherein generating the first seed key is performed by the peripheral device, where the peripheral device is the mobile, and the first seed key is the M-Key.

In reference to claim 5:

Patel (Column 2, lines 22-30) discloses a method wherein generating the first seed key includes:

- Using the public encryption key(A-Key) associated with the software component(AC/HLR) to select from a plurality of private encryption keys(SSDA, SSDB) associated with the peripheral device(The mobile);
- And summing the select private keys associated with the peripheral device, where SSDA and SSDB are combined.

In reference to claim 6:

Patel(Column 4, lines 1-10) discloses a method wherein establishing an encrypted link includes performing orthogonal encryption of data transmitted to and from the hardware controller, where the orthogonal encryption performed is a DES-CBC to provide a substantially orthogonal result.

In reference to claim 7:

Patel(Column 4, 51-62) & (Column 2, lines 56-57) discloses a method wherein including: Providing the public encryption key(A-key) associated with the peripheral device(Mobile) and a private decryption key(SSDA), associated with the software component(AC/HLR software), to the hardware component(AC/HLR hardware); Providing public key encryption between the hardware controller(HLR) and the peripheral device(Mobile), where the public key encryption is understood to be established between to AC/HLR and the mobile, as the purpose of Patel is to establish the keys to be used.

In reference to claim 8:

Patel(Column 4, lines 1-11) discloses a method wherein the orthogonal encryption is performed using an orthogonal encryption key, wherein the orthogonal encryption key is capable of changing dynamically, where the orthogonal encryption key is capable of changing whenever a DES-CBC encryption is performed on the A-key.

In reference to claim 9:

Patel(Column 4, lines 1-11) discloses a method wherein the orthogonal encryption is performed using an orthogonal transform function, wherein the orthogonal transform function is capable of changing dynamically, where the orthogonal transform function is classified as a PRF or pseudorandom function and is capable of changing dynamically from its pseudorandom nature.

In reference to claim 12:

Patel(Column 1, lines 55-59) & (Column 4, lines 1-11) discloses a method wherein the step of establishing further includes the first seed key being based upon the peripheral device and the information handling system, where the first seed key is based on the A-key, which is unique to the peripheral device and the information handling system.

In reference to claim 13:

Patel(Column 1, lines 55-59) & (Column 4, lines 1-11) discloses a method wherein the first seed key is unique to the peripheral device and the information handling system, where the first seed key is based on the A-key, which is unique to the peripheral device and the information handling system.

In reference to claim 14:

Patel discloses a hardware controller comprising:

- A bus connection to receive a first seed key(M-key) from a software component(software of the AC/HLR) within an information handling system(AC), where the M-key is received from the PRF function used to generate it. (Column 4, lines 1-10)
- A digital communications connector to connect to a peripheral device(mobile) and to receive a public encryption key from said peripheral device, where the digital communications connector allows for the wireless mobile connection.
- A first set of registers to store said first seed key, (M-key) said first seed key common to both said information handling system and the peripheral device, where the first register is the home location register, which acts as a communication conduit, or the Authentication Center. (Column 4, lines 1-11)
- A second register to store said public encryption key(A-key), where the second register is the Home location register. (Column 1, lines 55-59)
- A processing circuit to generate, using said first seed key and said public encryption key a second seed key different from said first seed key, said second seed key to encrypt communications between said software component and said

hardware controller, where the SSD is used in the encrypted data between the mobile and the system. (Column 2, lines 55-59)

Claim 15 is rejected for the same reasons as claim 5.

In reference to claim 16:

Patel(Column 1, lines 40-48) discloses a hardware controller wherein communications between said hardware controller(HLR) and said information handling system(AC) are performed over a system bus, where a system bus is inherent to the information systems necessary to transmit information. Examiner further maintains that a system bus is inherent to all desktop computer systems today.

Claim 21 is rejected for the same reasons as claim 6.

Claim 22 is rejected for the same reasons as claim 8

Claim 23 is rejected for the same reasons as claim 9

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 10, 11, 17-20, 24-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel.

In reference to claim 10:

Patel discloses all of claim 10 except a method wherein the hardware controller is a video controller.

The examiner takes official notice that it was well known to those of ordinary skill in the art that a type of hardware controller is a video controller.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a video controller, in order to extend cryptographic communications to that type of hardware controller.

In reference to claim 11:

Patel discloses all of claim 11 except a method wherein the peripheral device is a display device.

The examiner takes official notice that a display device was a well known peripheral device at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a display peripheral device as a peripheral device, in order to extend cryptographic communications to that peripheral entity.

In reference to claim 17:

Patel discloses all of claim 17 except a hardware controller wherein said system bus is a peripheral component interconnected bus.

The examiner takes official notice that PCI buses were well known to those of ordinary skill in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to disclose a system wherein the system bus was a PCI bus, to allow communications with other PCI devices.

In reference to claim 18:

Patel discloses all of claim 18 except a hardware controller wherein said digital communications connector is a digital video interface connector.

The examiner takes official notice that digital video interface connectors were a well known type of digital communications connector to those of ordinary skill in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to disclose a system that used digital video interface connectors in order to extend digital communications to digital video.

Claim 19 is rejected for the same reasons as claim 10.

Claim 20 is rejected for the same reasons as claim 11.

In reference to claim 24:

Patel discloses a processor coupled to a system bus:

- A collection of instructions to be stored and executed by said processor, said collection of instructions including instructions to establish an encrypted link between said system and a peripheral device(Mobile), wherein establishing said encrypted link includes generating a first seed key(M-key) common to both said peripheral device and said system, said collection of instructions further including instructions to deliver said first seed key to a peripheral controller, where the collection of instructions is the software executed establishes an encrypted link between the AC/HLR and the mobile through a session request. (Column 2, lines 27-35) to generate a first seed key, M-key common to both the peripheral and the system. (Column 4, lines 1-11)
- A peripheral controller including a bus connection to receive said first seed key(M-key), where the communications controller on the mobile receives the seed key from the PRF function (Column 4, lines 1-11)
- A digital communications link to connect to said peripheral device and to receive a public encryption key (A-key) from said peripheral device(Mobile), where key is received by the mobile through manufacturing. (Column 1, lines 55-59)
- A first set of registers to store said first seed key(M-key), where the visiting location register may store the M-key because it acts as a conduit of communication between the system and the mobile, or the Authentication Center, another registry where the M-key must be stored. (Column 4, lines 12-19)
- A second register to store said public encryption key(A-key), where the second register is the Home location register. (Column 1, lines 55-59)

- A processing circuit to generate, using said first seed key(M-key) and said public encryption key, a second seed key(SSD) different from said first seed key, said second seed key to encrypt communications between said system and said peripheral controller (Column 2, lines 20-30)

Patel fails to explicitly disclose memory coupled to said system bus for use by said processor.

The examiner takes official notice that memory coupled to a bus for use by a processor was well known at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to couple memory to a system bus to a processor in order to allow the processor to access the memory.

In reference to claim 25:

Patel discloses all of claim 25 except a system wherein said memory includes random access memory and read-only memory.

The examiner takes official notice that systems which include RAM and ROM were well known to those of ordinary skill in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to disclose a system that included RAM and ROM to allow the system to store data.

Claim 26 is rejected for the same reasons as claim 5.

In reference to claim 27:

Patel discloses a system wherein said public encryption key and said plurality of private encryption keys are located the mobile and the AC/HLR, and thereby inherently located in the memory of each device.

Claim 28 is rejected for the same reasons as claim 17.

Claim 29 is rejected for the same reasons as claim 18.

Claim 30 is rejected for the same reasons as claim 10.

Claim 31 is rejected for the same reasons as claim 11.

Claim 32 is rejected for the same reasons as claim 6.

Claim 33 is rejected for the same reasons as claim 8.

Claim 34 is rejected for the same reasons as claim 9.

In reference to claim 35:

Patel(Column 1, lines 55-60) discloses a system wherein the digital communications link is to receive a public encryption key from said peripheral device, where the peripheral device is the mobile, and to transmit encrypted digital data to said peripheral device, where the data transmitted the to the peripheral device is encrypted with session keys. (Column 2, lines 55-58)

Conclusion

8. The following prior art not relied upon is made of record:

US Patent 6,173,174 is a method for updating SSD and A-key entries in Mobile telephones.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

April 26th 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100